UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/532,988	04/28/2005	Hiromi Ebara	2005-0683A	3027

52349   7590   09/17/2008
WENDEROTH, LIND & PONACK L.L.P.
2033 K. STREET, NW
SUITE 800
WASHINGTON, DC 20006

EXAMINER
LOONAN, ERIC T

ART UNIT	PAPER NUMBER
2189	

MAIL DATE	DELIVERY MODE
09/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

<table>
<tr><td rowspan="2">Office Action Summary</td><td>Application No.
10/532,988</td><td>Applicant(s)
EBARA ET AL.</td></tr>
<tr><td>Examiner
ERIC LOONAN</td><td>Art Unit
2189</td></tr>
</table>

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>23 July 2008</u>.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-16</u> is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) <u>1 and 3-16</u> is/are rejected.
7)☒ Claim(s) <u>2</u> is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on <u>28 April 2005</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☒ All   b)☐ Some * c)☐ None of:
      1.☒ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)
1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

U.S. Patent and Trademark Office
PTOL-326 (Rev. 08-06)   Office Action Summary   Part of Paper No./Mail Date 20080911

DETAILED ACTION

This Office action is in response to applicant's remarks submitted 23 July 2008

based on application 10/532,988 originally filed 28 April 2005. **Claims 1-16** are

currently pending and have been considered below.

Specification

1.   The specification is objected to as failing to provide proper antecedent basis for

the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction

of the following is required: **Claim 16** recites a "nontamper resistant memory" without

providing a definition of the memory type in the specification.

Claim Objections

2.   **Claim 2** is objected to as being dependent upon a rejected base claim, but would

be allowable if rewritten in independent form including all of the limitations of the base

claim and any intervening claims.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148

USPQ 459 (1966), that are applied for establishing a background for determining

obviousness under 35 U.S.C. 103(a) are summarized as follows:

1.   Determining the scope and contents of the prior art.
2.   Ascertaining the differences between the prior art and the claims at issue.
3.   Resolving the level of ordinary skill in the pertinent art.
4.   Considering objective evidence present in the application indicating
     obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of

the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of

the various claims was commonly owned at the time any inventions covered therein

were made absent any evidence to the contrary. Applicant is advised of the obligation

under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was

not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g)

prior art under 35 U.S.C. 103(a).

4.   **Claims 1, 3, 6-14, and 16** rejected under 35 U.S.C. 103(a) as being

unpatentable over Nagamasa et al (US PGPub 2004/0177215) hereinafter known as

Nagamasa in view of Kawaura (US Patent 6,886,069).

Claim 1: Nagamasa teaches a semiconductor memory card comprising a tamper

resistant module that is tamper resistant (Fig 1, 150 – IC Card Chip and 120 –

Controller Chip) and a nontamper resistant memory that is a nonvolatile memory that is

not tamper resistant (Fig 1, 130 – Flash memory chip), wherein the tamper resistant

module includes: an internal memory having a usage area used by a program stored in

the tamper resistant module (Fig 26, 162 – EEPROM; Section [0043]); and a processing

unit (Fig 1, 120 – Controller Chip and Fig 26, 158 - CPU), wherein when requested by

the program, the processing unit is operable to (i) assign an area in the nontamper

resistant memory to the program (Section [0051]), and (ii) generate, on the internal

memory of the tamper resistant module, access information for the assigned area in the

nontamper resistant memory (Section [0052], Section [0055]) and wherein the assigned

area in the nontamper resistant memory is for a portion of confidential data to be written

in, the portion of confidential data being used by the program and read by referring to

the access information existing in the internal memory of the tamper resistant module

(Section [0051]). In **Claim 3**, Nagamasa teaches a semiconductor memory card

wherein the processing unit comprises: an assigning unit operable to assign, at a time

of the generation of the access information, an encryption key which the program uses

in accessing the assigned area in the nontamper resistant memory (Fig 23, 2321 – User

Certificate; Section [0055]); an encrypting unit operable, at a time of the program writing

data to the assigned area in the nontamper resistant memory, to encrypt the data (Fig

23, 2313; Section [0055]); and a decrypting unit operable, at a time of the program

reading data from the assigned area in the nontamper resistant memory, to decrypt the

data (Fig 23 – 2324; Section [0055]). In **Claim 6**, Nagamasa teaches a semiconductor

memory card wherein the nontamper resistant memory includes a first memory module

(Fig 1, 130 – Flash memory chip) and a second memory module (Fig 26, 160 – RAM),

and a unit of writing in the second memory module is smaller than a unit of writing in the

first memory module, and the second memory module stores file management data

(Section [0043]). In **Claim 8**, Nagamasa teaches a semiconductor memory card

wherein the internal memory of the tamper resistant module includes a first memory

module (Fig 26, 162 - EEPROM) and a second memory module (Fig 26, 160 – RAM),

and a unit of writing in the second memory module is smaller than a unit of writing in the

first memory module, and the second memory module stores file management data

(Section [0043]). In **Claims 7 and 9**, Nagamasa teaches a semiconductor memory card

wherein the second memory module is one of a Ferroelectric Random Access Memory

and a Magnetoresistive Random Access Memory (Fig 26, 160 – RAM). In **Claim 10**,

Nagamasa teaches a semiconductor memory card being a multi-application memory

card, wherein the program is one of a plurality of applications with which the memory

card is compatible, and the internal memory has a plurality of usage areas

corresponding one to one to the applications (Fig 21, multiple areas are assigned to

different processes; Section [0051]). In **Claim 11**, Nagamasa teaches a semiconductor

memory card wherein at a time of addition of one of the applications to the memory

card, the processing unit assigns an area to be used by the added application (Fig 21,

multiple areas are assigned to different processes; Section [0051]). In **Claim 12**,

Nagamasa teaches a semiconductor memory card wherein the assigned area is a file

system in which files are stored (Fig 21, 2130 – User File Area). In **Claim 13**,

Nagamasa teaches a semiconductor memory card wherein the tamper resistant module

includes a CPU that executes the program (Fig 1, 121 – CPU). In **Claim 14**, Nagamasa

teaches a semiconductor memory card including a host interface which is an interface

with a device connected to the memory card, wherein the host interface judges whether

a command from the device is an expansion command, and the program starts, if the

command is judged to be the expansion command (Section [0059]; DIO terminal 2544).

In **Claim 16**, Nagamasa teaches a controlling program in a semiconductor memory card

that comprises a tamper resistant module (Fig 1, 150 – IC Card Chip and 120 –

Controller Chip) and a nontamper resistant memory (Fig 1, 130 – Flash memory chip),

and that is executed by a CPU in the tamper resistant module, wherein the tamper

resistant module includes an internal memory having a usage area used by an

application stored in the tamper resistant module (Fig 26, 162 – EEPROM; Section

[0043]); wherein the controlling program is operable to (i) assign an area in the

nontamper resistant memory to the application (Section [0051]), and (ii) generate, on

the internal memory of the tamper resistant module, access information for the assigned

area in the nontamper resistant memory (Section [0055]), and wherein the assigned

area in the nontamper resistant memory is for a portion of confidential data to be written

in, the portion of confidential data being used by the program and read by referring to

the access information existing in the internal memory of the tamper resistant module

(Section [0051]).

In **Claims 1 and 16**, while Nagamasa discloses a ROM (Fig 26, 159) in the IC

card chip (Fig 26, 150), Nagamasa does not appear to explicitly disclose the contents of

the ROM nor a processing unit including a virtual machine and an operating system.

However, Kawaura discloses a ROM which stores program codes, including an

operating system (Col 4, Lines 14-19).

Nagamasa and Kawaura are analogous art because they are from the same field of endeavor of integrated circuit cards.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Nagamasa and Kawaura before him or her, to modify the ROM of Nagamasa to include program codes as taught by Kawaura.

A motivation for doing so would have been to install software on the non-rewriteable module.

Therefore, it would have been obvious to combine Nagamasa with Kawaura to obtain the invention as specified in the instant claims.

5.   **Claims 4 and 5** are rejected under 35 U.S.C. 103(a) as being unpatentable over Nagamasa and Kawaura in view of Madoukh (US PGPub 2001/0019614).

In **Claim 4**, Nagamasa and Kawaura disclose the semiconductor card of its parent claim.

In **Claim 5**, Nagamasa and Kawaura disclose the semiconductor card of its parent claim. Further, Nagamasa teaches semiconductor memory card wherein the internal memory stores a first area table indicating a location and a size of the usage area, the nontamper resistant memory stores a second area table indicating a location and a size of the assigned area in the nontamper resistant memory (Section [0051], Section [0052], Fig 21).

In **Claim 4**, Nagamasa and Kawaura do not appear to explicitly disclose a

semiconductor memory card wherein the processing unit further comprises: a receiving

unit operable to receive a security level from the program; and a storage unit that stores

values for different security levels, bit lengths of an encryption key, and encryption

methods, the bit lengths and encryption methods corresponding one-to-one to the

values, the encryption key assigned by the assigning unit is generated based on a bit

length corresponding to the received security level, and the encryption and decryption

by the encrypting unit and decrypting unit, respectively, are performed based on an

encryption method corresponding to the received security level.

In **Claim 5**, Nagamasa and Kawaura do not appear to explicitly disclose a

semiconductor memory card wherein the second area table being encrypted using a

predetermined encryption key, and the access information is a set of the predetermined

encryption key and information indicating a location of the second area table.

However, with respect to **Claim 4**, Madoukh teaches a receiving unit operable to

receive a security level from the program; and a storage unit that stores values for

different security levels (Section [0056]), bit lengths of an encryption key (Section

[0044], keys with extended lengths), and encryption methods (Section [0044], different

hashing algorithms), the bit lengths and encryption methods corresponding one-to-one

to the values, the encryption key assigned by the assigning unit is generated based on

a bit length corresponding to the received security level (Section [0045], encryption key

manager assigns keys per the user session), and the encryption and decryption by the

encrypting unit and decrypting unit, respectively, are performed based on an encryption method corresponding to the received security level (Section [0044]).

However, with respect to **Claim 5**, Madoukh teaches an encryption key manager (Section [0045]).

Nagamasa, Kawaura, and Madoukh are analogous art because they are from the same field of endeavor of data storage.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Nagamasa, Kawaura, and Madoukh before him or her, to modify the semiconductor card of Nagamasa and Kawaura to include the encryption methods as taught by Madoukh.

The motivation for doing so would have been to deploy the data security methods onto the semiconductor card.

Therefore, it would have been obvious to combine Nagamasa and Kawaura with Madoukh to obtain the invention as specified in the instant claims.

6.   **Claim 15** is rejected under 35 U.S.C. 103(a) as being unpatentable over Nagamasa and Kawaura in view of Deo et al (US Patent 5,721,781) hereinafter known as Deo.

In **Claim 15**, Nagamasa and Kawaura disclose the teachings of its parent claim and includes a plurality of file systems.

Nagamasa and Kawaura do not appear to explicitly disclose a secure level of each of the file systems being one of high, medium, and low, wherein a first file system

whose secure level is high is stored in the tamper resistant module, a second file

system whose secure level is low is stored in the nontamper resistant memory, and the

total area that is a combination of the usage area in the tamper resistant memory and

the assigned area in the nontamper resistant memory composes a third file system

whose secure level is medium.

However, Deo teaches an authentication system that utilizes different terminals

for different security levels (Col 10, Lines 42-67).

Nagamasa, Kawaura, and Deo are analogous art because they are from the

same field of endeavor of semiconductor card transactions.

At the time of the invention, it would have been obvious to one of ordinary skill in

the art, having the teachings of Nagamasa, Kawaura, and Deo before him or her, to

modify the semiconductor card of Nagamasa and Kawaura to include the authentication

system as taught by Deo.

The motivation for doing so would have been to assign different security levels to

data for the purpose of storing the data in different locations.

Therefore, it would have been obvious to combine Nagamasa and Kawaura with

Deo to obtain the invention as specified in the instant claims.

Allowable Subject Matter

7.   **Claim 2** is allowable over the prior art of record. The claim limitation sets forth

storage of area tables of a tamper resistant memory and a nontamper resistant memory

in the tamper resistant memory, keeping the location of the usage area secret (Page 3,

Lines 26-28 to Page 4, Lines 1-2 of applicant's specification).

Response to Arguments

Applicant's remarks filed 23 July 2008 based on Office Action mailed on 23 April

2008 have been fully considered below.

Claim Rejections under 35 U.S.C. § 103

8.   Applicant argues that the prior art of record fails to teach "generate, on the

internal memory of the tamper resistant module, access information for the assigned

area in the nontamper resistant memory". Applicant further notes that the controller

chip 120 of Nagamasa is able to access data that is temporarily stored in the flash

memory chip 130, and transmit such data to the IC card chip 150.

The Examiner has considered applicant's remarks, but is not persuaded by them

and maintains the rejection of record. The examiner maintains that data is stored on the

IC card chip 150 on EEPROM 162 as stated in the rejection of record.

9.   Applicant argues that the prior art of record fails to teach the claim limitations of

Claim 2.

The Examiner has considered applicant's remarks and is persuaded by them and

allowable if the claim is written in independent form.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ERIC LOONAN whose telephone number is (571)272-6994. The examiner can normally be reached on Monday-Friday, 7:30am-5:00pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Reginald Bragdon can be reached on (571) 272-4204. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Eric Loonan/
Examiner, Art Unit 2189

/Reginald G. Bragdon/
Supervisory Patent Examiner, Art Unit 2189